The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/14/2017

SUBJECT:
Multiple Vulnerabilities in Microsoft Office Could Allow for Remote Code Execution (MS17-014)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Office, the most severe of which could result in remote code execution if a user opens a specially crafted Microsoft Office file. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Microsoft Office: 2007, 2010, 2013, 2013 RT, 2016
- Microsoft Office: for Mac 2011, 2016 for Mac
- Microsoft Office Compatibility Pack SP3
- Microsoft Word Viewer
- Microsoft Excel Viewer
- Microsoft Lync for Mac
- Microsoft SharePoint Server: 2007, 2010, 2013
- Microsoft Office Web Apps: 2010, 2013

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Microsoft Office, the most severe of which could result in remote code execution if a user opens a specially crafted Microsoft Office file. The vulnerabilities are as follows:

- Multiple remote code execution vulnerabilities exist in Microsoft Office software when the Office software fails to properly handle objects in memory. (CVE-2017-0006, CVE-2017-0019, CVE-2017-0020, CVE-2017-0030, CVE-2017-0031, CVE-2017-0052, CVE-2017-0053)
- An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory. (CVE-2017-0027)
- A denial of service vulnerability exists when a specially crafted file is opened in Microsoft Office. (CVE-2017-0029)
- An information disclosure vulnerability exists when Microsoft Office software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory. (CVE-2017-0105)
- An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. (CVE-2017-0107)
- A security feature bypass exists when the Lync for Mac 2011 client fails to properly validate certificates. (CVE-2017-0129)

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:

https://technet.microsoft.com/library/security/MS17-014

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0006
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0019
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0020
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0027
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0029
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0030
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0031
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0052
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0053
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0105
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0107
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0129